Report di Laboratorio: Hacking Windows con Metasploit

Exploitation di Icecast e Post-Exploitation su Windows 10

Josh Van Edward D Abanico

22 gennaio 2026

Sommario

Il presente documento illustra le attività di Penetration Testing condotte contro una macchina target Windows 10. L'attività si concentra sullo sfruttamento di una vulnerabilità nel servizio Icecast per ottenere una sessione remota Meterpreter. Successivamente, vengono eseguite operazioni di post-exploitation quali l'identificazione dell'indirizzo IP della vittima e l'acquisizione di uno screenshot del desktop remoto.

Indice

1 Obiettivo dell'Esercitazione

L'obiettivo primario è ottenere il controllo remoto di un sistema Windows 10 sfruttando il software vulnerabile **Icecast**. Utilizzando il framework **Metasploit**, condurremo un attacco strutturato nelle seguenti fasi:

1. Selezione e configurazione del modulo di exploit per Icecast.
2. Esecuzione dell'attacco per ottenere una sessione **Meterpreter**.
3. Verifica dell'identità di rete (Indirizzo IP).
4. Acquisizione di prove tramite screenshot.

2 Analisi dello Scenario: Icecast

Il software oggetto dell'attacco è **Icecast**, un server per lo streaming multimediale open source, ampiamente utilizzato per creare radio online e distribuire contenuti audio/video. La versione installata sulla macchina target Windows 10 presenta una vulnerabilità critica nota (CVE-2004-1561).

2.1 Dettagli della Vulnerabilità

La vulnerabilità risiede in un errore di gestione della memoria (Buffer Overflow) durante il parsing degli header HTTP.

- **Natura del problema:** Il server non controlla adeguatamente la lunghezza dei dati inviati nel campo header della richiesta HTTP (in particolare il campo "Host" o header simili).
- **Meccanismo di exploit:** Inviando una richiesta appositamente modificata con un header eccessivamente lungo, è possibile sovrascrivere il buffer di memoria allocato e sovrascrivere il registro EIP (Instruction Pointer).
- **Conseguenza:** Questo permette all'attaccante di deviare il flusso di esecuzione del programma verso un codice arbitrario (payload), ottenendo così l'esecuzione di comandi remoti (RCE) con i privilegi dell'applicazione Icecast.

3 Fase 1: Selezione del Modulo Icecast

In questa prima fase, all'interno della console di Metasploit (`msfconsole`), è stato cercato e selezionato l'exploit specifico per la vulnerabilità di buffer overflow presente in Icecast.

Modulo utilizzato: `exploit/windows/http/icecast_header`

Di seguito viene mostrata la selezione del modulo e il controllo delle opzioni disponibili tramite il comando `show options`.

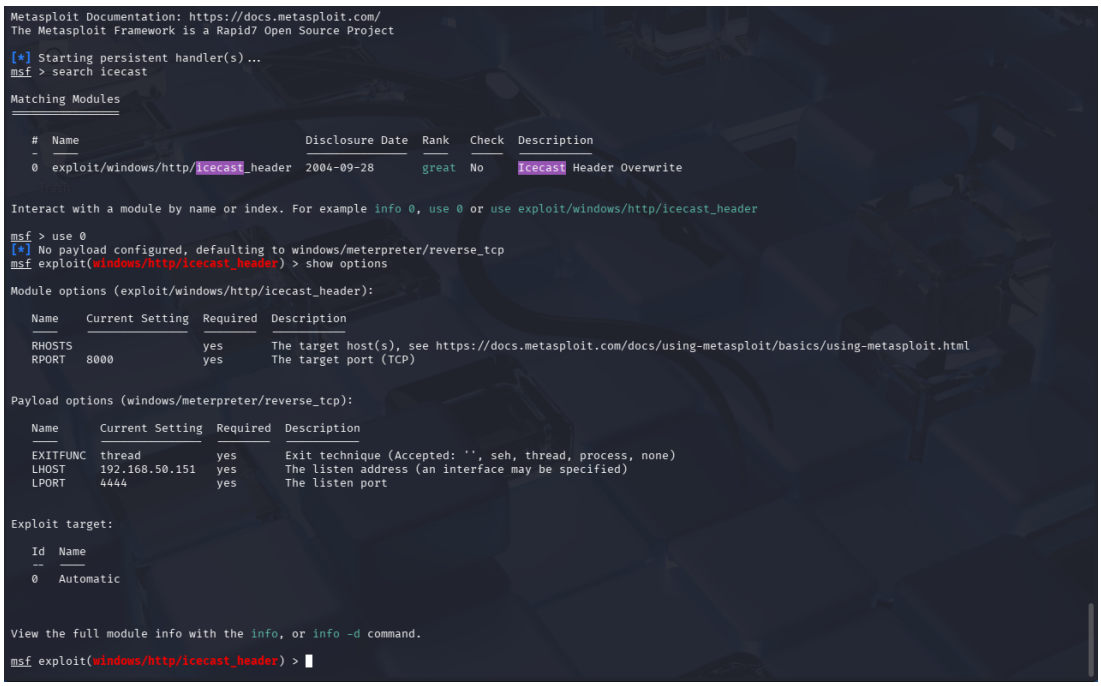

Figura 1: Selezione del modulo exploit Icecast Header.

4 Fase 2: Configurazione ed Exploitation

Una volta selezionato il modulo, si è proceduto alla configurazione dei parametri essenziali per stabilire la connessione inversa (Reverse TCP).

4.1 Configurazione dei Parametri

Sono stati impostati i seguenti valori:

- **RHOSTS**: Indirizzo IP della macchina target (Windows 10).
- **LHOST**: Indirizzo IP della macchina attaccante (Kali Linux).
- **LPORT**: Porta di ascolto (default 4444).

Lanciando il comando `exploit`, il payload è stato inviato con successo, aprendo una sessione **Meterpreter**.

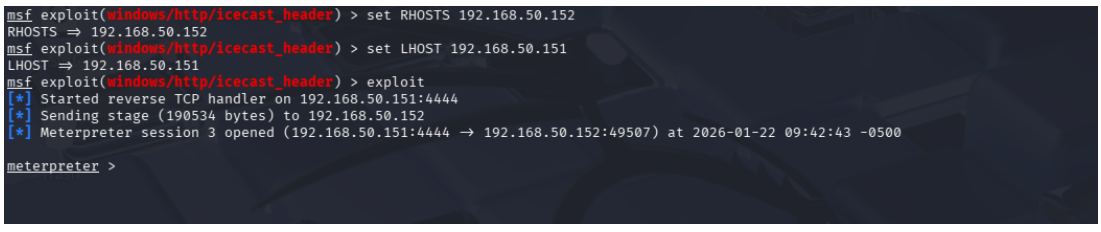

Figura 2: Esecuzione dell'exploit e apertura della sessione Meterpreter.

5 Fase 3: Post-Exploitation

Ottenuta la sessione Meterpreter, sono state eseguite le azioni richieste per verificare il controllo sulla macchina.

5.1 Verifica Indirizzo IP

Utilizzando il comando `ipconfig` all'interno della shell Meterpreter, è stata visualizzata la configurazione di rete della vittima per confermare l'indirizzo IP.

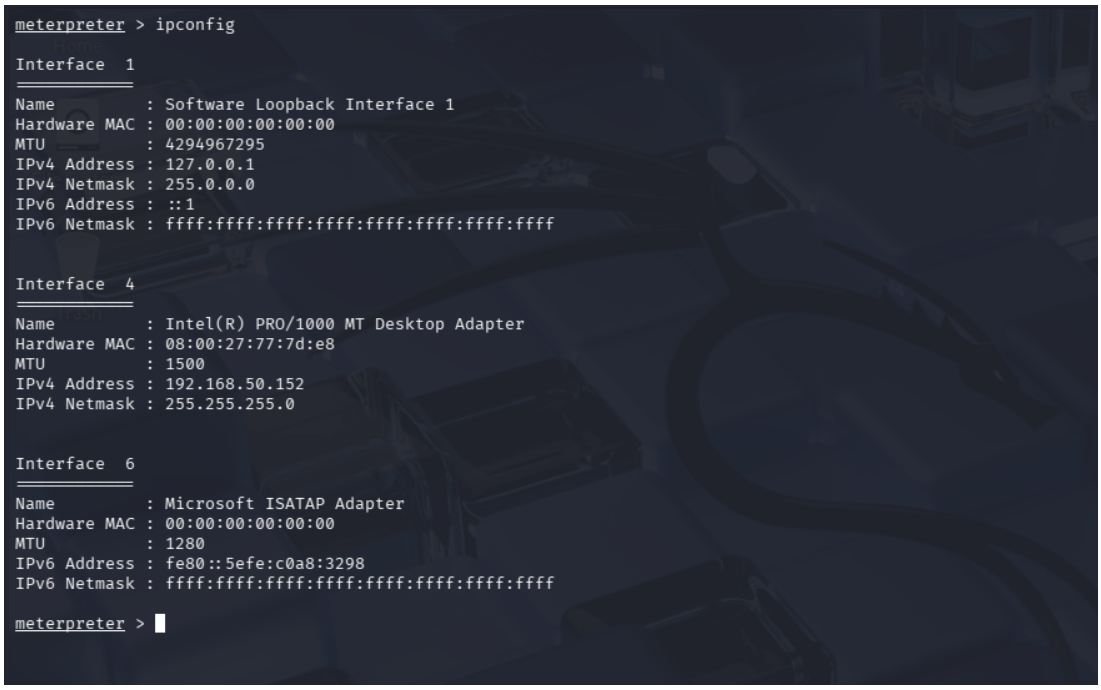

Figura 3: Visualizzazione dell'indirizzo IP della vittima.

5.2 Verifica Privilegi e File System

Successivamente, è stato verificato l'utente corrente con il comando `getuid` e visualizzato il contenuto della directory di lavoro (Icecast) tramite il comando `ls`.

Figura 4: Verifica utente (getuid).

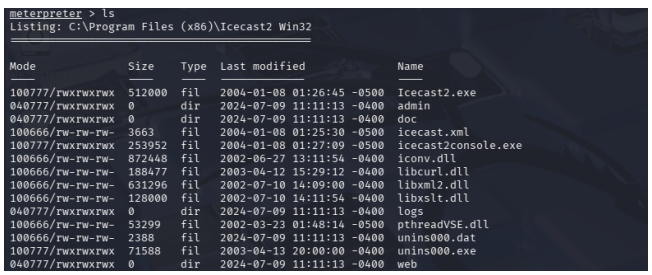

Figura 5: Listing dei file (ls).

5.3 Recupero Screenshot

Infine, è stato utilizzato il comando `screenshot` per catturare l'istantanea del desktop della macchina Windows 10, confermando la piena visibilità sul sistema.

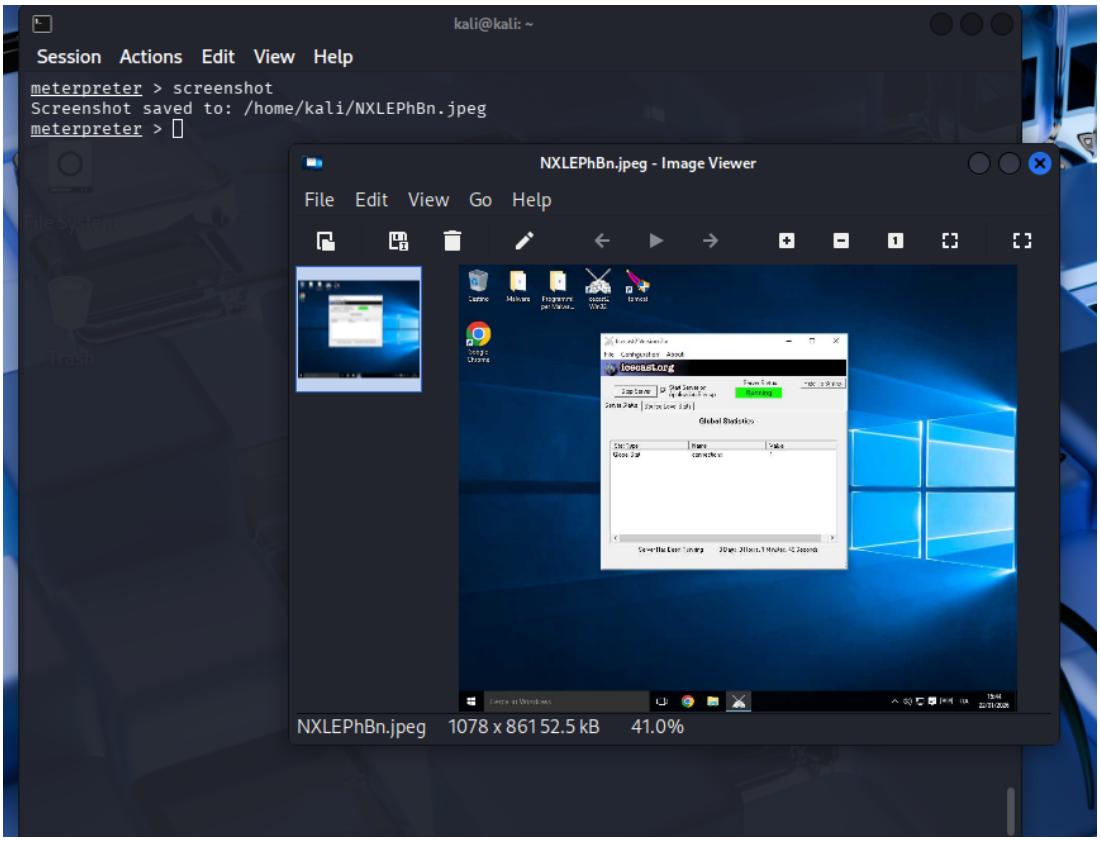

Figura 6: Esecuzione del comando screenshot e salvataggio file.

6 Conclusioni

L'esercitazione ha dimostrato come un software non aggiornato (Icecast) su un sistema Windows 10 possa fungere da vettore di ingresso per un attaccante. L'utilizzo di Metasploit ha permesso di automatizzare l'exploit, garantendo immediatamente una sessione Meterpreter stabile, tramite la quale è stato possibile esfiltrare informazioni sensibili (configurazione di rete) e monitorare l'attività dell'utente (screenshot).